# Insider attacks and RFID Privacy models

Ton van Deursen and Saša Radomirović

{ton.vandeursen, sasa.radomirovic}@uni.lu

University of Luxembourg

Financial support received from the Fonds National de la Recherche (Luxembourg)

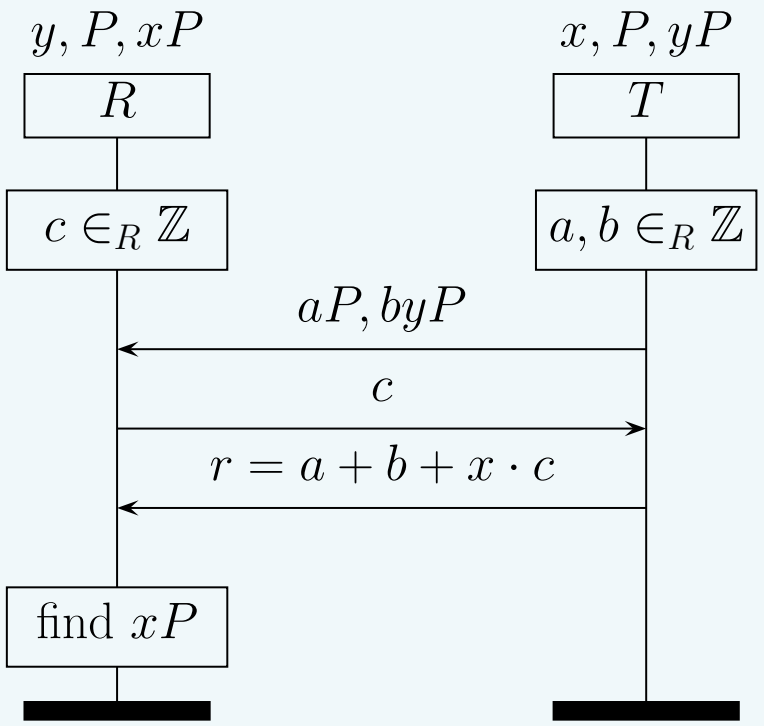
# Overview

In an insider attack the adversary uses a tag that is fully under his control.

His goal is to break the privacy/security of some other tag.

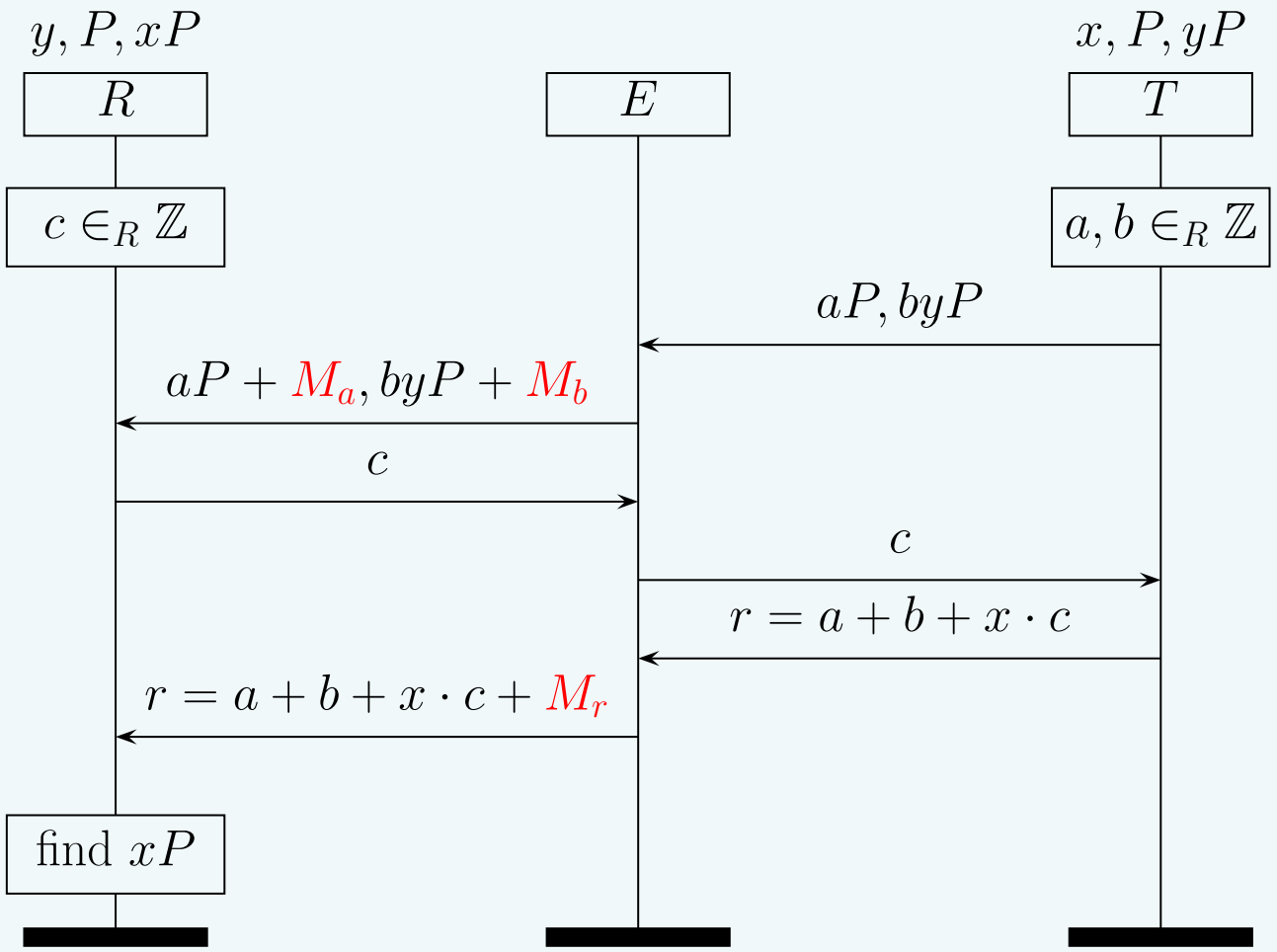
Insider attacks are relevant in public-key based protocols.

# Randomized Schnorr protocol




$$xP = (rP - aP - byP \cdot y^{-1})c^{-1}$$

# Man-in-the-middle attack



# Man-in-the-middle attack

Adversarial strategy:

- Observe two runs of a protocol for tags $x$ and $x'$: $aP, byP, c, r$ and $a'P, b'yP, c', r'$.
- Compute $M_a, M_b$ and $M_r$.
- Perform man-in-the-middle attack: if the reader accepts the tag $x = x'$ otherwise $x \neq x'$.

$M_a, M_b$ and $M_r$ need to satisfy:

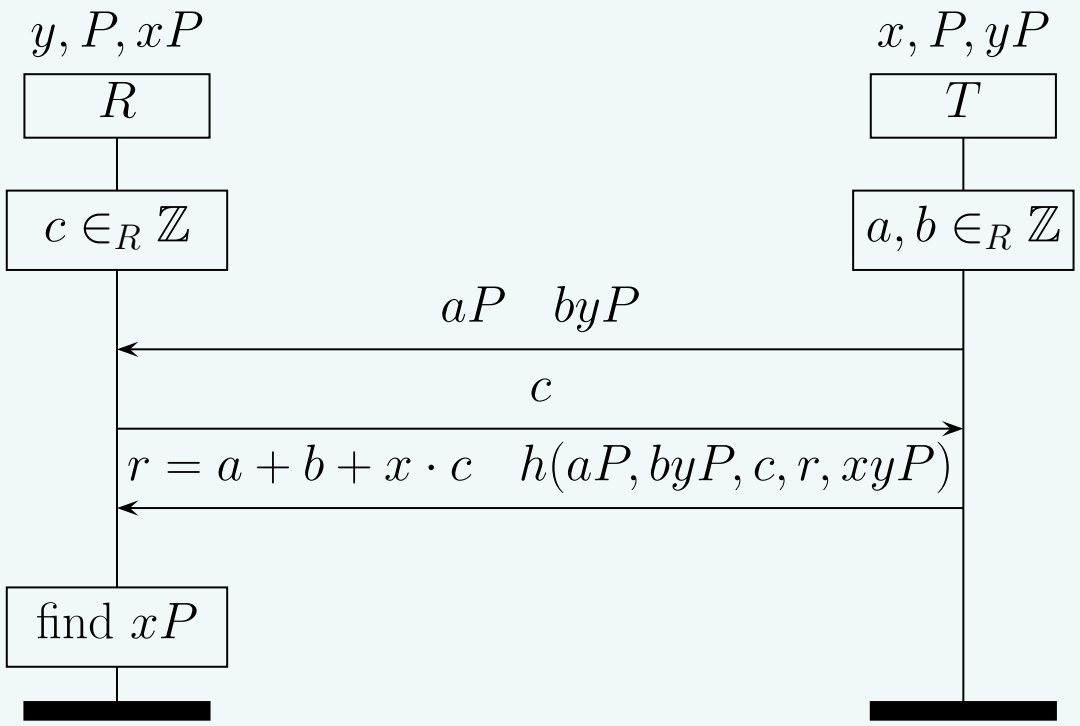
- $M_a = ca'P + c'aP$
- $M_b = c'byP + cb'yP$
- $M_r = c'r - cr' = (c'a - ca') + (c'b - cb') + (xcc' - x'c'c)$

# Why does this work?

RFID security requires that the reader accepts a legitimate tag only if the reader and tag have a matching conversation.

The randomized Schnorr protocol does not satisfy security.

# Randomized Schnorr protocol (hardened)



# Randomized Schnorr protocol (hardened)

The hardened randomized Schnorr protocol satisfies security due to the hash function.

The man-in-the-middle attack is no longer possible since the attacker does not know $xyP$.

An insider can compute the hash and can therefore still perform the attack.

# Implications

Vaudenay's adversary classes:

$$\begin{array}{ccccccc} \text{w-strong} & \Rightarrow & \text{w-destructive} & \Rightarrow & \text{w-forward} & \Rightarrow & \text{w-weak} \\ \Downarrow & & \Downarrow & & \Downarrow & & \Downarrow \\ \text{n-strong} & \Rightarrow & \text{n-destructive} & \Rightarrow & \text{n-forward} & \Rightarrow & \text{n-weak} \end{array}$$

A wide attacker can observe whether a protocol run ended successfully.

# Implications

Vaudenay's lemma (2007) still holds:

- Narrow-weak privacy + security $\Rightarrow$ wide-weak.
- Narrow-forward privacy + security $\Rightarrow$ wide-forward.

Ng et al's theorems (2008) no longer hold:

- Narrow-destructive privacy + security $\Rightarrow$ wide-destructive.
- Narrow-strong privacy + security $\Rightarrow$ wide-strong.

# Conclusions

Conclusions:

- There exist protocols that are vulnerable to insider attacks.
- Insider attacks are only relevant for public-key protocols.

Future work:

- Adapt privacy models for insider attacks.
- Find minimal conditions for absence of insider attacks.

Thank you!

`http://satoss.uni.lu/ton/`